Distributed Intrusion Response System

ABSTRACT

A system and method to respond to intrusions detected on a network system including attached functions and a network infrastructure. The system includes means for receiving from an intrusion detection function information about intrusions, a directory service function for gathering and reporting at least the physical and logical addresses of devices of the network infrastructure associated with the detected intrusions, and a plurality of distributed enforcement devices of the network infrastructure for enforcing policies responsive to the detected intrusions. A policy decision function evaluates the reported detected intrusions and makes a determination whether one or more policy changes are required on the enforcement devices in response to a detected intrusion. A policy manager function configures the distributed enforcement devices with the responsive changed policy or policies. Policy changes rules can vary from no change to complete port blocking on one or more identified enforcement devices associated with the detected intrusion, to redirecting the associated traffic including the intrusion and these policies may be modified or removed over time as warranted by network operation.